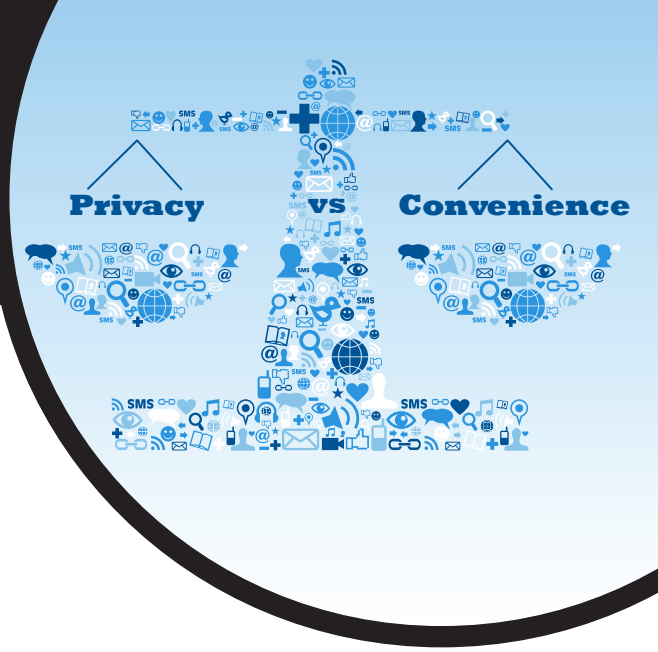
EMC

Privacy Index



Executive Summary

News headlines about Internet privacy are fueling a debate about how much access governments and businesses should have into the private activities, communications and behaviors of citizens and customers.

The EMC Privacy Index is a contribution to this important dialogue on Internet privacy. It was commissioned by EMC to better understand consumer perception about the need to protect personal privacy online and how that ranks as a consumer priority against the benefits of convenient online commerce and social media sharing, alongside other priorities such as the use of data analytics to prevent terrorist attacks and protect national security. EMC also sought to leverage the Privacy Index as a means to understand consumer attitudes globally around the fundamental question of responsibility. Whose responsibility is it to ensure the protection of consumers' digital privacy in an era of cloud and mobile computing, social media and Big Data analytics?

Against this backdrop, the Index provides a fascinating view into consumer attitudes on digital privacy, and the degree to which perspectives vary depending on geography as well as six behavioral personas that people take on when they go online to engage in a variety of common activities.

The Index ultimately reveals that privacy is a complex issue, with consumers exhibiting a number of behaviors that often appear to be directly at odds with their stated wants and beliefs.

Methodology

This study was conducted online through a quantitative survey of 15,000 respondents globally, with each sample designed to be nationally representative and weighted to gender and age. Margin of error for each country was +/- 3.1% and globally +/- 1%.

The Index was developed using metrics to assess "consumers' willingness to trade some privacy for more benefits or conveniences associated with digital technology."

The Privacy Personae

The results of the Privacy Index make clear that, depending on the type of activity being engaged in, people behave differently – giving rise to a number of online personas (or "Me's), each with different attitudes towards privacy. The six personas evaluated include:

> Social Me
Interaction with social media sites, email programs, text/SMS and other communications services.

> Financial Me
Interaction with banks and other financial institutions.

> Citizen Me
Interaction with government institutions.

> Medical Me
Interaction with doctors, medical institutions and health insurers.

> Employee Me
Interaction with employment-related systems and Web sites.

> Consumer Me
Interaction with online stores.

Viewpoints on privacy vary wildly depending on what online persona is affected. For instance, respondents reported that their "citizen" persona has the greatest willingness to forfeit privacy to gain protection from terrorists or criminal activity. Meanwhile, their "social" persona claims to be the least willing to give up privacy for greater social connectedness.

The Privacy Paradoxes

Three distinct, yet intertwined privacy paradoxes emerged as particularly significant, each with powerful implications for consumers, businesses and technology providers as they consider the issue of digital privacy.

First, the **"We Want It All" Paradox**: People worldwide are using technology at a high rate and place considerable value on the benefits offered by digital technology, yet few say they are willing to give up ANY of their privacy in exchange for the ability to keep receiving these benefits. This paradox applies not only to everyday consumer benefits, such as searching for nearby shops by enabling geo-location, but to more critical benefits to citizens such as protection from terrorist and/or criminal activity.

Attitudes are stronger in different parts of the world. In India, for example, consumers are much more inclined to trade privacy for conveniences, while German citizens are on the other end of the spectrum with an overwhelmingly allergic response to the notion of compromising any of their privacy. Respondents in other geographies also appear to lean towards a general unwillingness to relinquish their online privacy, despite placing a significant value on the benefits of the connected world. This presents a challenge for businesses and governments to strike the right balance between protecting individual privacy while delivering services as diverse as law enforcement protection and targeted e-commerce.

Second, the **"Take No Action" Paradox** tells us that while more than half of consumers have experienced a data breach where their privacy was potentially compromised, they are not taking basic measures to protect their information, such as changing passwords regularly and using password protection on mobile devices. Most believe it is the responsibility of the government, not the individual, to protect consumers' privacy through the creation of laws and regulations. Exacerbating this dilemma, the Index exposed a widespread lack of confidence in the organizations charged with protecting privacy, whether businesses or governments. Although consumers view these institutions as possessing adequate skills for protecting privacy, they view them as lacking the ethics and transparency needed to safeguard the privacy of individuals, pointing to an erosion of trust in institutions and businesses.

Third, the "Social Sharing" Paradox confirms that the overwhelming majority of consumers worldwide are actively sharing information via social media channels. More than 400 million Tweets were shared daily in 2012, and more than 1 billion share personal information on Facebook.3 However, respondents do so while giving low confidence ratings in the abilities and ethics of institutions to protect the privacy of individuals' social personas.

Key Findings

The "We Want It All" Paradox

- Irrespective of persona and type of benefit, people have very little willingness to trade privacy for the benefits of digital technology:
  - > 91% of respondents value the benefit of "easier access to information and knowledge" that digital technology affords. Yet only 45% would be willing to trade some of their privacy for that easier access.
  - > And interestingly, in light of news associated with surveillance, 85% of respondents value "the use of digital technology for protection from terrorist and/or criminal activity"; however, only 54% would be willing to trade some of their privacy for greater protection.
- When compared with other countries, consumers in India are the most willing to trade their privacy for better services, with 48% expressing willingness.
- Unsurprisingly, citizens of Germany, a nation very protective of privacy, are the least willing to trade their privacy: 78% of Germans are unwilling to make the trade-off.

Value Conveniences & Willingness To Trade Privacy For Conveniences

Global total sample

The "Take No Action" Paradox

- Despite more than half of all respondents reporting having experienced a data breach (email account hacked; mobile device lost or stolen; social media account hacked; and more), many say they are not taking measures to protect themselves:
  - > 62% say they don't change passwords regularly.
  - > 33% say they don't customize privacy settings on social networks.
  - > 39% say they don't use password-protection on mobile device.
- Respondents listed businesses using, selling or trading personal data for financial gain (51%) and the lack of government attention (31%) among the top risks to the future of privacy, but "a lack of personal oversight and attention from regular people like me" was ranked very low (11%).
- Meanwhile, there remains low consumer confidence that governments and businesses possess the skills and ethics to adequately safeguard the privacy of data.
  - > On average, only 58% of respondents believe that governments and businesses have the skills needed to protect individuals' privacy, and only 49% felt organizations have adequate ethics and transparency to protect individuals' privacy.
- 87% believe there should be laws to prohibit businesses from buying and selling data without consumers' opt-in consent.

The "Social Sharing" Paradox

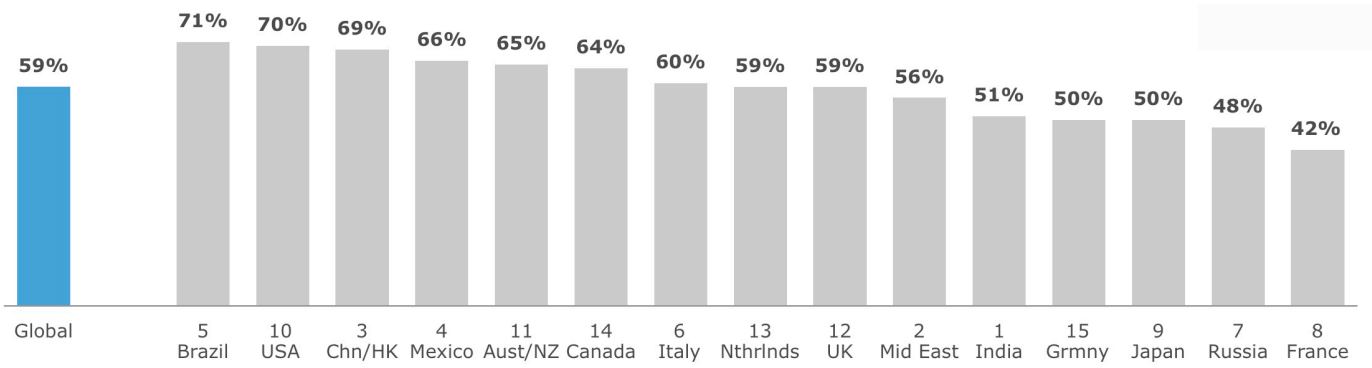
- The vast majority of consumers (84%) claim they don't like anyone knowing anything about themselves or their habits unless they make a decision themselves to share that information.
- And with almost one-fifth of respondents claiming to have suffered a hacked social media account (17%), it stands to reason that social media users would exercise caution.
- Yet this is where internet users freely upload personally identifiable information and photographs multiple times per day.
  - > For instance, according to the EMC Digital Universe study, there were more than 1 billion Facebook users in 2012, and over 400 million Tweets were posted daily.
  - > The use of social media to connect with people was cited by 68% of respondents as among the top five online activities worldwide.
- Contributing to the paradox, users are sharing their personal data despite:
  - > Respondents expect their privacy on social media will be most difficult to maintain in the next five years.
  - > A belief among consumers that the skills and ethics of institutions to safeguard information on social media is appallingly low;
    - + Just 51% claim to have confidence in the skills of these providers to protect our data, and just 39% claim to have confidence in those organizations' ethics.

A Dismal Global Privacy Outlook

- The confidence people have in their levels of privacy is falling over time.
  - > Compared to a year ago, 59% of global respondents feel they have less privacy now - perhaps correlating to the white-hot global stage to which the privacy debate has ascended within the past year.
    - + Brazil and the United States reported the highest percentage of respondents who feel they have less privacy now, with 71% and 70% respectively.
    - + France is the only country with a majority (56%) that disagrees with the statement that they have less privacy now than a year ago.

Question: "I Have Less Privacy Now Than I Did A Year Ago"

Agree%



- Nearly all respondents expect privacy will be more elusive in the next five years, demonstrating an expectation that people will see their privacy increasingly diminish in future years
  - > 74% of consumers expect that privacy will be more difficult to maintain in the next five years.
  - > Among the top perceived risks to the future of privacy are financial fraud (64%) and businesses selling data (51%), but there is also concern about those who are perceived to be responsible for protecting data.
    - + 35% view a major risk as "incompetence on the part of those who should protect privacy and secure personal data".
    - + 31% cite "lack of government attention" (laws, regulation, funding, enforcement) when it comes to the privacy of personal data.
- The privacy outlook across all types of data is dim.
  - + Respondents cite a high level of future concern across all types of digital data, with the greatest concern pertaining to social data.
    - + 78% are concerned about the future of privacy of their social data (social me).
    - + 76% are concerned about the future of privacy of their citizen (citizen me) and financial data (financial me).
    - + 75% are concerned about the future of their consumer data (consumer me).
  - > Privacy outlook is somewhat less pessimistic for "medical me" and "employee me," though it is still grim.
    - + 72% are concerned about the future of privacy of their medical data.
    - + 66% are concerned about the future of privacy of their employee data.

Regional Highlights

North Americans (Americans and Canadians) believe they have less privacy today than a year ago and expect this trend to continue over the five years

- The United States and Canada are low on the spectrum when it comes to their willingness to trade their privacy for greater convenience, with the US coming in 10th and Canada coming in 14th out of the 15 countries surveyed.
- In both countries, overall confidence in privacy is low:
  - > 70% of Americans and 64% of Canadians believe that they have less privacy now than they did a year ago.
  - > 85% of Americans and Canadians expect privacy will be more difficult to maintain in the next five years.
- Consumers in both the US and Canada have lower confidence in organizations' ethics than organizations' skills in protecting their privacy.

Willingness to trade Internet benefits for privacy varied greatly in EMEA

- Countries in EMEA varied greatly when it came to their willingness to trade their privacy for greater convenience
- The EMEA countries polled in the EMC Privacy Index, ranked in order of willingness to trade their privacy for greater convenience, include:
  - Italy (6 out of 15)
  - Russia (7 out of 15)
  - France (8 out of 15)
  - UK (12 out of 15)
  - Netherlands (13 out of 15)
  - Germany (15 out of 15)
- An extraordinarily high 77% of Germans said that they would not be willing to trade privacy for convenience. However, simultaneously:
  - 63% say they do not change their passwords regularly;
  - 27% say they don't customize privacy settings on social networks; and,
  - 41% say they don't have password protections on their mobile devices.

- When it comes to their "Citizen Me" and "Medical Me" personas, Italians are more willing than the global average to share their data (8% higher for Citizen Me and 12% higher for Medical Me)
- 46% of people in France say they are unlikely to read privacy statements, and 71% say they do not change their passwords regularly.

The majority of APAC countries (with the exception of Japan) showed a greater willingness to trade their privacy for greater Internet benefits

- With the exception of Japan and Australia, which landed lower in the spectrum, most APAC countries showed a higher than average willingness to trade their privacy for greater convenience.
- The APAC countries polled in the EMC Privacy Index, ranked in order of their willingness to trade their privacy for greater convenience, include:
  - India (1 out of 15)
  - Middle East (2 out of 15)
  - China and Hong Kong (3 out of 15)
  - Japan (9 out of 15)
  - Australia and New Zealand (11 out of 15)
- 48% of people in India said that they would be willing to share data, making it the country most likely (both in the APAC region as well as globally) to trade privacy for greater convenience.
  - People in India are almost twice as likely to share data with financial institutions (66% of people in India as compared with 38% globally);
  - 70% of Indians (as compared with an average of 50% globally) are willing to share their data with government bodies; and,
  - 77% of Indians are confident in organizations' skills, and 73% are confident in organizations' ethics in protecting their privacy.

EMC's Position on Privacy

- EMC favors protecting the privacy and civil liberties of individuals on the Internet. We believe the potential of Cloud Computing and the use of Big Data to address society's most urgent challenges will be accelerated by the protection of information assets and trust in the Cloud.
- EMC is committed to complying with applicable privacy and data security laws. EMC supports a comprehensive privacy and data security framework to protect personal information With more than 64,000 employees in 86 countries worldwide, EMC supports efforts to harmonize privacy and security standards around the world.
- EMC provides technologies and services to enterprise customers primarily. EMC also provides data storage, sharing and information protection solutions to consumers. EMC has internal privacy and data security policies that require the protection of information it collects from customers, employees and partners.